T S6/5/1

6/5/1
DIALOG(R)File 347:JAPIO

06569949 **Image available**
SYSTEM AND METHOD FOR DIRECTORY ACCESS CONTROL BY COMPUTER

PUB. NO.: 2000-155715 [JP 2000155715 A]
PUBLISHED: June 06, 2000 (20000606)
INVENTOR(s): OKUMA YOSHIYUKI
KASUGA YASUNARI
NAKAJIMA YUSAKU
APPLICANT(s): NTT DATA CORP
APPL. NO.: 10-329188 [JP 98329188]
FILED: November 19, 1998 (19981119)
INTL CLASS: G06F-012/14; G06F-012/00; G06K-019/073

ABSTRACT

PROBLEM TO BE SOLVED: To make flexible and independent access between directories in a hierarchical directory structure.

SOLUTION: For directories 11 and 13, security properties 11A and 13A, security statuses 11S and 13S, inheritance masks 11IM and 13IM, and open masks 11RM and 13RM are prepared. In the security properties 11A and 13A, in what security statuses 11S and 13S the directories are allowed to be accessed are defined as to respective access right levels. The security statuses 11S and 13S show what kind of key a person inputted for authentication to try to access the directories. The inheritance masks 11IM and 13IM prescribe what bit can be inherited when the security status are inherited from other directories to their directories. The open masks 11RM and 13RM prescribe what bit can be inherited when the security levels are inherited from their directories to other directories.

?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－155715
（P2000－155715A）
(43)公開日　平成12年６月６日(2000.6.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ	５Ｂ０１７
12/00	５３７	12/00	５３７Ａ	５Ｂ０３５
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｂ０８２

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

(21)出願番号　特願平10－329188

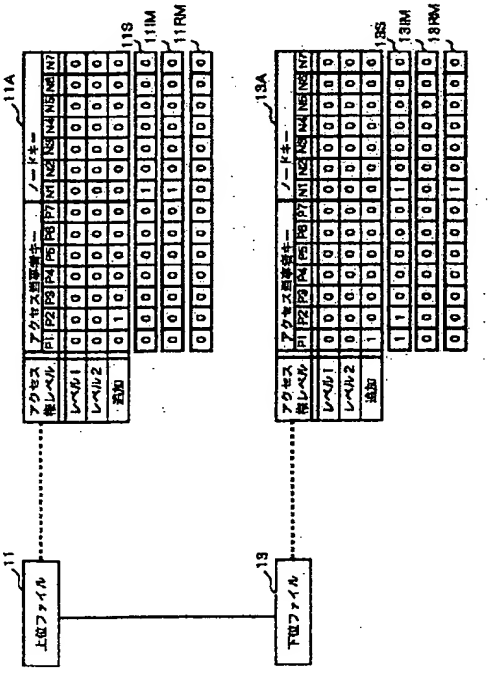
(22)出願日　平成10年11月19日(1998.11.19)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　大熊　喜之
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　春日　靖成
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095371
弁理士　上村　輝之

最終頁に続く

(54)【発明の名称】　コンピュータのディレクトリアクセス制御システム及び方法

(57)【要約】
【課題】　階層状のディレクトリ構造において、ディレクトリ間のアクセスの融通性と独立性とを両立させる。
【解決手段】　各ディレクトリ１１、１３に、セキュリティ属性１１Ａ、１３Ａと、セキュリティステータス１１Ｓ、１３Ｓと、継承マスク１１ＩＭ、１３ＩＭと、公開マスク１１ＲＭ、１３ＲＭとが用意されている。セキュリティ属性１１Ａ、１３Ａには、各アクセス権レベルについて、当該ディレクトリのセキュリティステータス１１Ｓ、１３Ｓがどのようになっていれば当該ディレクトリのアクセスを許すかが定義されている。セキュリティステータス１１Ｓ、１３Ｓには、当該ディレクトリにアクセスしようとする者がどの種別のキーを入力して認証を行ったかを示している。継承マスク１１ＩＭ、１３ＩＭは、他のディレクトリから自ディレクトリへセキュリティステータスを継承するときに、継承できるビットがどれであるかを規定している。公開マスク１１ＲＭ、１３ＲＭは、自ディレクトリから他のディレクトリへセキュリティステータスを継承するときに、継承できるビットがどれであるかを規定している。



1

【特許請求の範囲】

【請求項１】　複数のディレクトリの各々に関して、認証結果を反映したセキュリティステータスと、前記セキュリティステータスがどのような内容であれば自ディレクトリへのアクセスを許すかを規定したセキュリティ属性と、他のディレクトリのセキュリティステータスを自ディレクトリのセキュリティステータスへ継承するときの条件を規定した継承マスクと、

着目しているディレクトリのセキュリティステータスへ、他のディレクトリのセキュリティステータスを継承させるときに、前記他のディレクトリのセキュリティステータスのうち前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる継承制御部と、

前記着目しているディレクトリのアクセスが要求されたときに、前記着目しているディレクトリのセキュリティ属性とセキュリティステータスとの所定の論理演算の結果に基づいて、前記着目しているディレクトリのアクセスを許可するか否かを決定するアクセス制御部とを備えたコンピュータのディレクトリアクセス制御システム。

【請求項２】　各ディレクトリに関して、自ディレクトリのセキュリティステータスを他のディレクトリのセキュリティステータスへ継承するときの条件を規定した公開マスクを更に備え、

前記継承制御部が、前記他のディレクトリのセキュリティステータスのうち、前記他のディレクトリの公開マスクに合致し且つ前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる請求項１記載のシステム。

【請求項３】　複数のディレクトリの各々に関して、認証結果を反映したセキュリティステータスと、前記セキュリティステータスがどのような内容であれば自ディレクトリへのアクセスを許すかを規定したセキュリティ属性と、他のディレクトリのセキュリティステータスを自ディレクトリのセキュリティステータスへ継承するときの条件を規定した継承マスクとを有したコンピュータシステムにおいて、

着目しているディレクトリのセキュリティステータスへ、他のディレクトリのセキュリティステータスを継承させるときに、前記他のディレクトリのセキュリティステータスのうち前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる継承制御ステップと、

前記着目しているディレクトリのアクセスが要求されたときに、前記着目しているディレクトリのセキュリティ属性とセキュリティステータスとの所定の論理演算の結果に基づいて、前記着目しているディレクトリのアクセスを許可するか否かを決定するアクセス制御ステップとを有したコンピュータのディレクトリアクセス制御方法。

2

【請求項４】　前記コンピュータシステムは、各ディレクトリに関して、自ディレクトリのセキュリティステータスを他のディレクトリのセキュリティステータスへ継承するときの条件を規定した公開マスクを更に有し、

前記継承制御ステップが、前記他のディレクトリのセキュリティステータスのうち、前記他のディレクトリの公開マスクに合致し且つ前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる請求項３記載の方法。

【請求項５】　複数のディレクトリの各々に関して、認証結果を反映したセキュリティステータスと、前記セキュリティステータスがどのような内容であれば自ディレクトリへのアクセスを許すかを規定したセキュリティ属性と、他のディレクトリのセキュリティステータスを自ディレクトリのセキュリティステータスへ継承するときの条件を規定した継承マスクとを有したコンピュータシステムにおいて、

着目しているディレクトリのセキュリティステータスへ、他のディレクトリのセキュリティステータスを継承させるときに、前記他のディレクトリのセキュリティステータスのうち前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる継承制御ステップと、

前記着目しているディレクトリのアクセスが要求されたときに、前記着目しているディレクトリのセキュリティ属性とセキュリティステータスとの所定の論理演算の結果に基づいて、前記着目しているディレクトリのアクセスを許可するか否かを決定するアクセス制御ステップとを有したコンピュータのディレクトリアクセス制御方法、をコンピュータに実行させるためのプログラムを担持したコンピュータ読取可能な記録媒体。

【請求項６】　前記コンピュータシステムは、各ディレクトリに関して、自ディレクトリのセキュリティステータスを他のディレクトリのセキュリティステータスへ継承するときの条件を規定した公開マスクを更に有し、

前記継承制御ステップが、前記他のディレクトリのセキュリティステータスのうち、前記他のディレクトリの公開マスクに合致し且つ前記着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、前記着目しているディレクトリのセキュリティステータスに継承させる請求項５記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータによる情報記憶場所（ディレクトリ）へのアクセスを制御す

る技術に関わり、特に、多目的利用型のＩＣカードにおけるディレクトリの追加や削除の権利を管理するのに好適な情報アクセス管理技術に関する。

【０００２】

【従来の技術】コンピュータシステムでは、ファイルやフォルダなどの多数の論理的な記憶場所（ディレクトリ）を記憶領域内に形成し、ディレクトリにより記憶情報を整理し分類して管理している。複数のディレクトリは階層状の構成に組むことができる。例えば、図１に示すように、第１階層のあるファイル（又はフォルダ）１の中に、第２階層の幾つかのファイル（又はフォルダ）３、５を入れ、第２階層のあるファイル５の中に第３階層のファイル７を入れるというようにである。

【０００３】階層状のディレクトリ構造において、異なる階層のディレクトリのうちの階層の浅い側を「上位」、深い側を「下位」と、この明細書では形容する。例えば図１において、ファイル１はファイル３、５より上位であり、ファイル７はファイル５より下位である。最も上位のディレクトリは「ルートディレクトリ」と呼ばれる。着目しているディレクトリに至るためのルートディレクトリからの経路（ディレクトリの系列）を、その着目したディレクトリの「パス」と呼ぶ。例えば図１において、ファイル７のパスは「ファイル１－ファイル５－ファイル７」である。

【０００４】さて、コンピュータシステムの一種にＩＣカードがあり、ＩＣカード内の記憶領域もディレクトリにより管理される。単一の用途（例えば、一つの企業が提供する一種類のサービス）にしか利用できないＩＣカードが知られているが、一方、複数の用途（例えば、複数の企業が提供する多種類のサービス）に利用できる多目的利用型ＩＣカードも知られている。多目的利用型ＩＣカード内には、各利用目的毎に別個のディレクトリが構築される。例えば、図１において、Ａ社のサービスに使用するためにファイル３が形成され、Ｂ社のサービスに使用するためにファイル５が形成される。

【０００５】多目的利用型ＩＣカードでは、原則的に、Ａ社のサービスマシンはＡ社のサービス用のディレクトリにだけアクセスすることができ、他社のサービス用のディレクトリにはアクセスできないよう、各社及び各マシンのアクセス権を制御する必要がある。

【０００６】アクセス権を制御する従来の方法として、図１に示すように、各ディレクトリ１、３、５、７毎に固有のセキュリティ属性１Ａ、３Ａ、５Ａ、７Ａ及びセキュリティステータス１Ｓ、３Ｓ、５Ｓ、７Ｓを設定して、セキュリティ属性とセキュリティステータスの論理演算から、アクセスを許すか否かを決める方法が知られている。

【０００７】すなわち、図１の例では、各ディレクトリ１、３、５、７のセキュリティ属性１Ａ、３Ａ、５Ａ、７Ａには、７種別のアクセス当事者キー「Ｐ１」～「Ｐ７」及び７種別のノードキー「Ｎ１」～「Ｎ７」の各々に関して、３種類のアクセス権レベルの各アクセスが可能であるか否かが規定されている。ここで、「アクセス当事者キー」とは、そのディレクトリにアクセスしようとする者（例えば、サービス提供会社）がカードに入力するアクセスキーであり、また、「ノードキー」とは、そのアクセスに使用されるマシン（例えば、サービス提供会社の各カードリーダライタ）がカードに入力するアクセスキーである。各キー種別に該当するキーの具体的番号は、各ディレクトリ１、３、５、７毎に個別に設定することができる。

【０００８】図１に示した例では、ファイル１のセキュリティ属性５Ａには、例えばレベル「追加」のアクセス権（例えば、当該ファイル１の直下に、新たな下位のファイルを追加したり削除したりできる権利）に関し、キー種別「Ｐ１」に値「１」が設定され、他のキー種別には値「０」が設定されている。これは、当該ファイル１をカレントディレクトリとするアクセスコマンドを発した当事者が、当該ファイル１におけるキー種別「Ｐ１」に該当するアクセス当事者キーを入力して認証を行うと、当該ファイル１に対する「追加」のアクセスが許可されることを意味する。また、ファイル７のセキュリティ属性７Ａには、例えばレベル「書換」のアクセス権（例えば、当該ファイル７の書換えができる権利）に関し、キー種別「Ｐ２」と「Ｎ１」に値「１」が設定され、他のキー種別には値「０」が設定されている。これは、当該ファイル７におけるキー種別「Ｎ１」に該当するノードキーを持ち、かつ「Ｐ２」該当するアクセス当事者キーを持つマシンを用いて、当該ファイル７をカレントディレクトリとするアクセスコマンドを発した当事者が、キー種別「Ｐ２」のアクセス当事者キーを入力して認証を行えば、当該ファイル７の「書換」のアクセスが許可されることを意味する。

【０００９】各ディレクトリ１、３、５、７のセキュリティステータス１Ｓ、３Ｓ、５Ｓ、７Ｓは、そのディレクトリをカレントディレクトリとするアクセスを開始する際の認証時に、そのアクセス当事者及びマシンからキー種別に該当するキーが入力されたかを示すものである。例えば、図１では、ファイル５のセキュリティステータス５Ｓは、キー種別「Ｐ１」に関して値「１」が設定され、他のキー種別に関して値「０」が設定されている。これは、キー種別「Ｐ１」に該当するアクセス当事者キーのみが入力されたことを意味する。

【００１０】各ディレクトリ１、３、５、７についてのアクセス権の制御は、各ディレクトリのセキュリティ属性とセキュリティステータスとの論理演算により行う。その論理演算には何種類もあるが、簡単な一例を挙げれば、セキュリティ属性とセキュリティステータスとの論理積を計算して、この論理積の中の何れかのビットが「１」であれば（要するに、セキュリティ属性で

「１」が立っているキー種別に該当するキーで認証が行われれば）アクセスを許可するというものである。例えば図１の例では、ファイル５に着目すると、そのセキュリティステータス５Ｓには「Ｐ１」のビットに「１」が立っており（つまり、「Ｐ１」のキーで認証が行われている）、セキュリティ属性１Ａの「追加」に関するビット列でも「Ｐ１」のビットに「１」が立っているから、「追加」のアクセスが許可される。このように、各ディレクトリのアクセス制御はセキュリティ属性とセキュリティステータスとに基づいて行われる。

【００１１】更に、従来のアクセス制御では、あるディレクトリをカレントディレクトリとするアクセスに関して成立したセキュリティステータスが、他のディレクトリをカレントディレクトリとする別のアクセスのセキュリティステータスにも一定の規則に従って継承されるようになっている。その継承の規則は複雑であるが、それに基づく簡単な一例を挙げると、あるディレクトリ（例えば、ファイル５）をカレントディレクトリとする第１のアクセスに関して成立した当該カレントディレクトリ（ファイル５）に関するセキュリティステータスが、このカレントディレクトリのパス上のより上位のディレクトリ（例えば、ファイル１）をカレントディレクトリとする第２のアクセスにおける当該上位のディレクトリ（ファイル１）に関するセキュリティステータスにもそのまま継承される。例えば、第１のアクセスでファイル５に関して成立したセキュリティステータス５Ｓ「１０００００　００００００」が、第２のアクセスにおけるファイル１のセキュリティステータス１Ｓにそのまま継承され、ファイル１のセキュリティステータス１Ｓも「１０００００　００００００」となる。

【００１２】このように、あるディレクトリのセキュリティステータスを別のディレクトリにも継承させる理由は、ＩＣカードサービスの運用上の都合から、異なるディレクトリ間でのアクセスの融通性をもたせること（つまり、必要に応じて、あるディレクトリ用のアクセスキーを用いるだけで、他のディレクトリへのアクセスも可能にすること）が必要だからである。

【００１３】例えば、図１では、ファイル５のセキュリティステータス５Ｓがファイル１のセキュリティステータス１Ｓに継承されて「Ｐ１」のビットに「１」が立っている。このように継承が生じても、図１の例の場合には、ファイル１のセキュリティ属性１Ａでは「Ｐ１」のビットに「１」が立っていないので、ファイル１に関しては何のアクセスも許可されない。しかし、もし予めファイル１のセキュリティ属性１Ａの「追加」の「Ｐ１」のビットに「１」が設定されていたならば、上記継承によって、ファイル１に関する「追加」のアクセスが許可されることになる。このように、各ディレクトリのセキュリティ属性の設定の仕方によって、他のディレクトリからのセキュリティステータスの継承を反映させたり反

映させなかったりして、他のディレクトリのキーしか知らない者に対して、自ディレクトリへのアクセスを許可したり拒否したりという制御ができるのである。

【００１４】

【発明が解決しようとする課題】上述した従来技術によると、セキュリティステータスの継承を行うようにしたことの副作用として、異なるディレクトリ間でアクセスの独立性を保つこと（つまり、あるディレクトリのキーしか知らない者に対して、その者がアクセスしてはならない特定の他のディレクトリへのアクセスを絶対に許さないこと）が完全にはできないという問題が生じている。

【００１５】例えば、図１において、ファイル５用のキー種別「Ｐ１」のキーを入力してファイル５について「追加」のアクセスを許可された者が、次に、ファイル５の直下に新しいディレクトリ、例えばファイル７を追加して、このファイル７に関してキー種別「Ｐ２」のキーキーを新たに作成し、このファイル７にアクセスするためにその「Ｐ２」のキーを入力したとする。すると、このファイル７に関して「Ｐ２」のキーが入力された結果が、ファイル７のパス上にあるファイル５やファイル１のセキュリティステータスに継承されて、ファイル５やファイル１のセキュリティステータスは参照番号５Ｓ´、１Ｓ´で示すようにキー種別「Ｐ２」のビットにも「１」が立つことになる。その結果、本来許可してはいけないファイル１についての「追加」のアクセスが許可されるので、例えばファイル１の直下にある他のファイル３に対する削除などのアクセスが可能になってしまう。

【００１６】このように、従来技術では異なるディレクトリ間でのアクセスの融通性とアクセスの独立性とを両立させることができない。

【００１７】多目的利用型ＩＣカードでは、ユーザ毎に利用するサービスが異なる可能性が高い。そのため、ＩＣカード内に各サービスのディレクトリを作成する方法として、ユーザが個々のサービスの利用を開始する都度に、当該サービス用のディレクトリを、当該サービスの提供会社などの手によって追加していくという方法が採用されるであろう。しかし、ディレクトリ間の独立性が確実に保てないと、新規にディレクトリを追加した会社が、他の会社のディレクトリにもアクセスできるようになる可能性が生じる。

【００１８】従って、本発明の目的は、階層状のディレクトリ構造において、ディレクトリ間のアクセスの融通性と独立性とを両立できるようにすることにある。

【００１９】

【課題を解決するための手段】本発明に従うコンピュータのディレクトリアクセス制御システムは、複数のディレクトリの各々に関して、認証結果を反映したセキュリティステータスと、セキュリティステータスがどのよう

な内容であれば自ディレクトリへのアクセスを許すかを規定したセキュリティ属性と、他のディレクトリのセキュリティステータスを自ディレクトリのセキュリティステータスへ継承するときの条件を規定した継承マスクとを有している。そして、着目しているディレクトリのセキュリティステータスへ、他のディレクトリのセキュリティステータスを継承させるときに、他のディレクトリのセキュリティステータスのうち、着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、着目しているディレクトリのセキュリティステータスに継承させる。そして、着目しているディレクトリのアクセスが要求されたときに、着目しているディレクトリのセキュリティ属性とセキュリティステータスとの所定の論理演算の結果に基づいて、その着目しているディレクトリのアクセスを許可するか否かを決定する。

【００２０】このシステムによれば、継承マスクに設定した条件によって、他のディレクトリから自ディレクトリへセキュリティステータスを継承する度合いを制御することができる。例えば、特定のキーに関する認証結果だけを継承するように設定することもできるし、何も継承しないように設定することもできる。この継承マスクによる継承制御により、ディレクトリ間のアクセスの融通性を生じさせることも、アクセスの独立性を確保することもできる。

【００２１】好適な実施形態では、各ディレクトリに関して、自ディレクトリのセキュリティステータスを他のディレクトリのセキュリティステータスへ継承するときの条件を規定した公開マスクが更に用意される。そして、継承制御では、他のディレクトリのセキュリティステータスのうち、当該他のディレクトリの公開マスクに合致し且つ着目しているディレクトリの継承マスクに規定された条件に合致した事項だけを、着目しているディレクトリのセキュリティステータスに継承させる。

【００２２】本発明は、ＩＣカードにおけるディレクトリのアクセス制御に好適であるが、ＩＣカード以外の種々のタイプのコンピュータでも採用することができる。

【００２３】本発明を実施するためのコンピュータプログラムは、ディスク型ストレージ、半導体メモリおよび通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。

【００２４】

【発明の実施の形態】図２は、本発明の一実施形態にかかるＩＣカードにおける階層ディレクトリのアクセス制御のための構成を示す。

【００２５】コンピュータの記憶領域では多数のファイル（又はフォルダ）が階層構造に組まれ得るが、図２ではその階層構造中で上位、下位の関係にある２つのファイル１１、１３のみを抽出して示している。従って、図示の上位ファイル１１の更に上位には、図示しない別のファイルが存在し得るし、上位ファイル１１の直下には、図示の下位ファイル１３以外に図示しない別のファイルが存在し得る。また、下位ファイル１３の更に下位にも、図示しない別のファイルが存在し得る。

【００２６】カード内のファイル１１、１３の各々は、従来技術のそれと同様の意味を持つセキュリティ属性１１Ａ、１３Ａとセキュリティステータス１１Ｓ、１３Ｓを有する他、さらに、継承（inherit）マスク１１ＩＭ、１３ＩＭと、公開（release）マスク１１ＲＭ、１３ＲＭとを更に有する。これら２種類のマスクは、異なるディレクトリ間でのセキュリティステータスの継承を制御するためのものである。ここで、あるディレクトリから他のどのディレクトリへセキュリティステータスを継承できるかを決める規則は、従来技術と同様であってもよいし、異なっていてもよいが、この実施形態ではとりあえず、下位ファイル１３をカレントディレクトリとするアクセスで成立した下位ファイル１３のセキュリティスタス１３Ｓは、この下位ファイル１３のパス上にある上位ファイル１１をカレントディレクトリとするアクセスにおいて、その上位ファイル１１のセキュリティステータス１１Ｓへ継承されることとする。

【００２７】各ファイル１１、１２の継承マスク１１ＩＭ、１３ＩＭは、他ファイルから自ファイルへとセキュリティステータスを継承する場合に、他ファイルのセキュリティステータスに対して適用されるマスクである。例えば、図２の例では上位ファイル１１の継承マスク１１ＩＭはキー種別「Ｎ１」のビットにのみ「１」が立っており、他のキー種別のビットは全て「０」である。これは、他のファイル（例えば下位ファイル１３）からこの上位ファイル１１へセキュリティステータスを継承する場合に、他ファイルのセキュリティステータスのうちキー種別「Ｎ１」のビットのみを継承し（つまり、他ファイルのステータスの「Ｎ１」のビットが「１」であれば、自ファイルのステータスの「Ｎ１」のビットも「１」になる）、他のキー種別のビットは継承しない（つまり、他ファイルのステータスの「Ｎ１」以外のビットが「１」であっても、自ファイルのそれは「１」にならない）ことを意味する。

【００２８】各ファイル１１、１２の公開マスク１１ＲＭ、１３ＲＭは、自ファイル１１、１３から他ファイルへセキュリティステータスを継承する場合に、自ファイルのセキュリティステータスに対して適用されるマスクである。例えば、図２の例では下位ファイル１３の継承マスク１３ＲＭはキー種別「Ｎ１」のビットにのみ「１」が立っており、他のキー種別のビットは全て「０」である。これは、この下位ファイル１３から他のファイル（例えば上位ファイル１１）へとセキュリティステータスを継承する場合に、自ファイル１３のセキュリティステータスのうちキー種別「Ｎ１」のビットのみを継承し（つまり、自ファイル１３のステータス１３Ｓの「Ｎ１」のビットが「１」であれば、他ファイルのそ

れも「１」になる）、他のキー種別のビットは継承しない（つまり、自ファイル１３のステータス１３Ｓの「Ｎ１」以外のビットが「１」であっても、他ファイルのそれは「１」にならない）ことを意味する。

【００２９】セキュリティステータスの継承の制御とディレクトリへのアクセスの制御は次のように行う。すな＊わち、第１のディレクトリにアクセスした者が、次に第１のディレクトリのセキュリティステータスを継承する第２のディレクトリにアクセスする場合、継承制御プロセスが、第２のディレクトリのセキュリティステータスを、

「第２のディレクトリのセキュリティステータス」
＝「第１のディレクトリのセキュリティステータス」ＡＮＤ
「第１のディレクトリの公開マスク」ＡＮＤ
「第２のディレクトリの継承マスク」

によって計算する。そして、アクセス制御プロセスが、この第２のディレクトリのセキュリティステータスとセキュリティ属性とを、従来技術と同様に論理計算することによって、第２のディレクトリにアクセスを許すか否かを決定する。

【００３０】例えば、図２の例では、下位ファイル１３※

「上位ファイルのセキュリティステータス１１Ｓ」
＝「下位ファイル１３のセキュリティステータス１３Ｓ」ＡＮＤ
「下位ファイル１３の公開マスク１３ＲＭ」ＡＮＤ
「上位ファイル１１の継承マスク１１ＩＭ」
＝「１１００００　１０００００」ＡＮＤ
「００００００　１０００００」ＡＮＤ
「００００００　１０００００」
＝「００００００００　１００００００」

と計算する。つまり、下位ファイル１３のセキュリティステータス１１Ｓのうち上位ファイル１３へ継承されるビットは、下位ファイル１３の公開マスク１３ＲＭと上位ファイル１１の継承マスク１１ＩＭの双方で「１」が立っているビット、つまりキー種別「Ｎ１」のビットのみである。こうして、上位ファイル１１のセキュリティステータス１１Ｓは「００００００００　１０００００」となる。図２の例では、上位ファイル１１のセキュリティ属性１１Ａでは、どのアクセス権レベルについても、キー種別「Ｎ１」のビットに「１」が立っていないので、上記した下位ファイル１３からの継承によっては、上位ファイル１１に関して何のアクセスも許可されないことになる。

【００３１】一方、もし、下位ファイル１３の公開マスク１３ＲＭと上位ファイル１１の継承マスク１１ＩＭの双方において、「Ｐ２」のビットに「１」が設定されていれば、下位ファイル１３からの継承により上位ファイル１１のセキュリティステータス１１Ｓでは「Ｐ２」にビットに「１」が立って、上位ファイル１１のセキュリティ属性１１Ａの「追加」の値と一致することになるので、上位ファイル１１に関して「追加」のアクセスが許可されることになる。

【００３２】以上のように、自ディレクトリの継承マスクによって、他ディレクトリから自ディレクトリへのセキュリティステータスの継承の度合いを制限することができる。また、自ディレクトリの公開マスクによって、

※のセキュリティステータス１３Ｓは「１１００００００００００００」となっている。この下位ファイル１３にアクセスして図示のセキュリティステータス１３Ｓを成立させた者が、次に上位ファイル１１にアクセスしようとする時、継承制御プロセスは、その上位ファイル１１のセキュリティステータス１１Ｓを、

自ディレクトリから他ディレクトリへのセキュリティステータスの継承の度合いを制限することができる。この２つのマスクの設定を巧みに組み合わせることで、異なるディレクトリ間でアクセスの融通性を生じさせることも、アクセスの独立性を確保することもできる。例えば、他のディレクトリからアクセスされる可能性を皆無にしたい場合、図２の下位ファイル１３のように、自ディレクトリの継承マスク１３ＩＭを全て「０」に設定しておけばよい。また、自ディレクトリから他ディレクトリへのアクセスの可能性を無くしたい場合は、図２の上位ファイル１１のように、自ディレクトリの公開マスク１１ＲＭを全て「０」に設定しておけばよい。

【００３３】以上、本発明の一実施形態を説明したが、上記の実施形態はあくまで本発明の説明のための例示であり、本発明を当該実施形態にのみ限定する趣旨ではない。従って、本発明は、上記実施形態以外の様々な形態でも実施することができる。例えば、上記実施形態では１つのディレクトリに１つの継承マスクと１つの公開マスクを用意したが、他の実施形態として、１つのディレクトリに、上位ディレクトリとの間の継承に関する継承マスク及び公開マスクと、下位ディレクトリとの間の継承に関する別の継承マスク及び公開マスクとを用意する方法や、更に別の実施形態として、１つのディレクトリに、他のディレクトリの各階層別に独立した継承マスク及び公開マスクを用意する方法や、更にまた別の実施形態として、１つのディレクトリに、他のディレクトリの

11　　12

各種類別に（例えば、ファイルかフォルダか、特定アプリケーションの専用ファイルか共用ファイルか、どのようなアクセス権があるファイルかなどに応じて）独立した継承マスク及び公開マスクを用意する方法なども採用し得る。また、公開マスクを設けずに、継承マスクだけを設けた実施形態も考え得る。

【図面の簡単な説明】

【図１】従来のＩＣカードにおける階層ディレクトリのアクセス制御のための構成を示すブロック図。

【図２】本発明の一実施形態にかかるＩＣカードにおける階層ディレクトリのアクセス制御のための構成を示すブロック図。

【符号の説明】

１１　上位のファイル（上位のディレクトリ）

１３　下位のファイル（下位のディレクトリ）

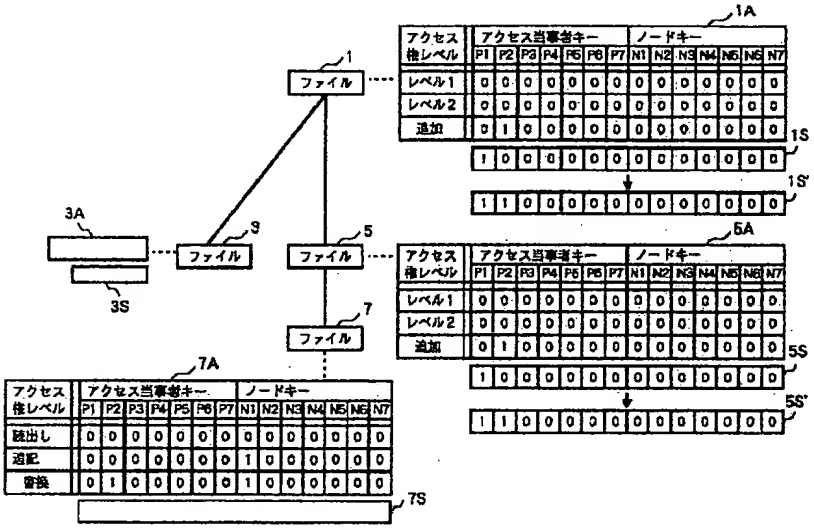
１１Ａ、１３Ａ　セキュリティ属性

１１Ｓ、１３Ｓ　セキュリティステータス

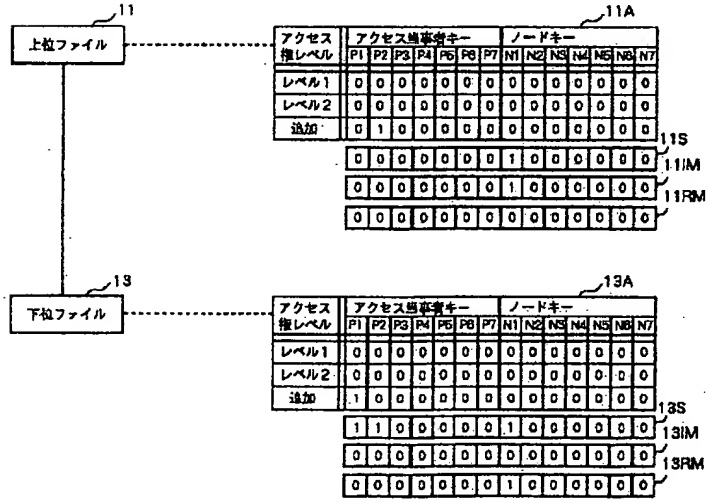
１１ＩＭ、１３ＩＭ　継承マスク

１１ＲＭ、１３ＲＭ　公開マスク

【図１】



【図２】



フロントページの続き

(72)発明者 中島 雄作
東京都江東区豊洲三丁目３番３号 株式会
社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5B017 AA01 BA06 BB06 CA14 CA16
5B035 AA13 BB09 CA29 CA38
5B082 EA01 EA11 GA13 JA08